EXHIBIT A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Auterinen.	
U.S. Patent No.:	7,423,962	Attorney Docket No.: 35548-0133IP1
Issue Date:	September 9, 2008	
Appl. Serial No.:	10/487,252	
Filing Date:	June 19, 2003	
Title:	REDUNDANCY AND LOAD BALANCING IN A TELECOM-MUNICATION UNIT AND SYSTEM	

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 7,423,962 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

EXHIBITS

EX1001	U.S. Patent No. 7,423,962 to Auterinen ("the '962 Patent")
EX1002	Prosecution History of the '962 Patent
EX1003	Declaration of Nathaniel J Davis, Ph.D.
EX1004	U.S. Patent No. 6,885,633 to Mikkonen ("Mikkonen")
EX1005	Knight, et. al., Request for Comment 2338, VIRTUAL ROUTER REDUNDANCY PROTOCOL (1998) ("RFC 2338")
EX1006	U.S. Patent No. 5,983,274 to Hyder et al. ("Hyder")
EX1007	Declaration of Sandy Ginoza
EX1008	Zwieback, High Availability Firewall/VPN with VRRP, LOGIN: THE MAGAZINE OF USENIX & SAGE
EX1009-1099	Reserved
EX1100	Complaints filed in *WSOU Investments LLC v. Huawei Technologies Co., Ltd., et al*., Case Nos. 6:20-cv-00889, 6:20-cv-00891-00893, 6:20-cv-00916-00917 (W.D. Tx.)
EX1101	Scheduling Order (Document 29), *WSOU Investments LLC v. Huawei Technologies Co., Ltd., et al*., Case Nos. 6:20-cv-00889-00893, 6:20-cv-00916-00917 (W.D. Tx.)
EX1102	Huawei's Stipulation served in *WSOU Investments LLC v. Huawei Technologies Co., Ltd., et al*., Case No. 6:20-cv-00917 (W.D. Tx.)

LISTING OF CLAIMS

Claim Element	Language
[1.P]	A method, comprising:
[1.a]	maintaining one or more logical nodes in each of first and second parallel physical cluster nodes configured to transmit data, wherein the first cluster node is a redundancy unit to the second cluster node and vice versa,
[1.b]	forming load allocation alternatives of the logical nodes, wherein the first logical node of the load allocation alternative resides in the first cluster node and the second logical node resides in the second cluster node, wherein the first logical node is active and the second logical node on standby or vice versa, and
[1.c]	performing, when a cluster node malfunctions, a switchover of the load allocation alternatives, the active logical nodes of which reside in the faulty cluster node, by changing their logical nodes from standby to active and the active logical nodes to standby,
[1.d]	wherein a network element in a communications system comprising the first and second cluster nodes is backed-up,
[1.e]	the method also comprising defining an individual external routing address for each load allocation alternative, on the basis of which data is transmitted to the network element.
[2]	A method as claimed in claim 1, wherein the load in the network element is distributed between the cluster nodes that comprise active logical nodes.
[3]	A method as claimed in claim 1, wherein traffic in the network element is distributed between the cluster nodes that comprise logical nodes.
[4]	A method as claimed in claim 1, wherein traffic in the network element is distributed on the basis of a specific load allocation plan between the cluster nodes that comprise logical nodes.
[5.a]	A method as claimed in claim 1, wherein information is further maintained on a primary and secondary cluster node associated with the load allocation alternative,
[5.b]	wherein data is transmitted to the primary cluster node and after a switchover of a load allocation alternative, data is

	transmitted to the secondary cluster node of the load allocation alternative.
[6]	A method as claimed in claim 1, wherein also a switchover of a load allocation alternative is performed such that after the switchover, data is transmitted through a physical interface of the backup cluster node to the redundancy unit of the cluster node.
[8]	A method as claimed claim 1, wherein said logical nodes are software-associated components of the cluster nodes.
[9.P]	A system, comprising:
[9.a]	a network element that comprises at least first and second parallel physical cluster nodes capable of transmitting data, wherein the first cluster node is configured to serve as a redundancy unit to the second cluster node and vice versa,
[9.b]	wherein the system is configured to: maintain logical nodes at least in the first and second cluster node,
[9.c]	form load allocation alternatives of the logical nodes such that the first logical node of the load allocation alternative resides in the first cluster node and the second logical node in the second cluster node, wherein the first logical node is active and the second on standby or vice versa, and;
[9.d]	perform, when a cluster node malfunctions, a switchover of the load allocation alternatives, the active logical nodes of which reside in the faulty cluster node, by changing the logical nodes from standby to active and the active logical nodes to standby;
[9.e]	wherein the system is configured to define for each load allocation alternative an individual external routing address, on the basis of which data is transmitted to the network element.
[10]	A system as claimed in claim 9, wherein the system is configured to distribute the load in the network element between the cluster nodes comprising active logical nodes.
[11.a]	A system as claimed in claim 9, wherein the system is configured to maintain information on a primary and secondary cluster node associated with the load allocation alternative,

[11.b]	wherein data is transmitted to the primary cluster node and, after a switchover, data is transmitted to the secondary cluster node of the load allocation alternative.
[12]	A system as claimed in claim 9, wherein the system is configured to perform a switchover of the load allocation alternative in such a manner that after the switchover, data is transmitted through a physical interface of the backup cluster node to the redundancy unit of the cluster node.
[18.P]	A apparatus comprising:
[18.a]	a first routine configured to maintain logical nodes at least first and the second parallel physical cluster nodes, capable of transmitting data, whereby the first cluster node is a redundancy unit to the second cluster node and vice versa,
[18.b]	a second routine configured to form load allocation alternatives of the logical nodes such that the first logical node of the load allocation alternative resides in the first cluster node and the second logical node resides in the second cluster node, wherein the first logical node is active and the second on standby or vice versa, and
[18.c]	a third routine configured to change, when a cluster node malfunctions, the load allocation of the logical nodes of the load allocation alternatives, the active logical nodes of which reside in the faulty cluster node, by changing the logical nodes from standby to active and the active nodes to standby,
[18.d]	wherein the apparatus also comprises a fourth routine configured to define an individual external routing address for each load allocation alternative, on the basis of which data is transmitted to the network element.
[19]	An apparatus as claimed in claim 18, wherein the apparatus comprises a fourth routine configured to distribute the load in the network element between the cluster nodes that comprise active logical nodes.
[20]	An apparatus as claimed in claim 18, wherein [sic] also comprises a fifth routine configured to distribute traffic in the apparatus between the cluster nodes that comprise logical nodes.
[21]	An apparatus as claimed in claim 18, wherein it also comprises a sixth routine configured to distribute traffic in the

	apparatus on the basis of a specific load allocation plan between the cluster nodes that comprise the logical nodes.
[22.a]	An apparatus as claimed in claim 18, wherein said first routine is also configured to maintain information on a primary and a secondary cluster node associated with the load allocation alternative,
[22.b]	wherein data is transmitted to the primary cluster node, and after a switchover, data is transmitted to the secondary cluster node of the load allocation alternative.
[23]	An apparatus as claimed in claim 18, wherein the apparatus also comprises an eighth routine configured to change load allocation wherein, after the switchover of a load allocation alternative, data is transmitted through a physical interface of the backup cluster node to the redundancy unit of the cluster node.
[24]	An apparatus as claimed in claim 18, wherein the apparatus also comprises a ninth routine configured to transmit data by using a routing address defined for the load allocation alternative even after a switchover of the load allocation alternative.
[40.P]	An apparatus, comprising:
[40.a]	a processor configured to:
[40.b]	maintaining logical nodes at least in first and second parallel physical cluster nodes capable of transmitting data, wherein the first cluster node is a redundancy unit to the second cluster node and vice versa,
[40.c]	form load allocation alternatives of the logical nodes such that the first logical node of the load allocation alternative resides in the first cluster node and the second logical node resides in the second cluster node, wherein the first logical node is active and the second on standby or vice versa, and,
[40.d]	change, when a cluster node malfunctions, the load allocation of the logical nodes of the load allocation alternatives, the active logical nodes of which reside in the faulty cluster node, by changing the logical nodes from standby to active and the active nodes to standby,
[40.e]	wherein the processor is configured to define an individual

	external routing address for each load allocation alternative, on the basis of which data is transmitted to the network element.
[41]	An apparatus as claimed in claim 40, wherein the processor is configured to distribute the load in the apparatus between the cluster nodes that comprise active logical nodes.
[42]	An apparatus as claimed in claim 40, wherein the processor is configured to distribute the traffic in the apparatus on the basis of a specific load allocation plan between the cluster nodes that comprise logical nodes.
[43]	An apparatus as claimed in claim 40, wherein the processor is configured to distribute the traffic in the apparatus on the basis of a specific load allocation plan between the cluster nodes that comprise logical nodes.
[44.a]	An apparatus as claimed in claim 40, wherein said the processor is configured to maintain information on a primary and a secondary cluster node associated with the load allocation alternative,
[44.b]	wherein data is transmitted to the primary cluster node and after a switchover, data is transmitted to the secondary cluster node of the load allocation alternative.
[45]	An apparatus as claimed in claim 40, wherein the processor is configured to load allocation in such a manner that after the switchover of a load allocation alternative, data is transmitted through a physical interface of the backup cluster node to the redundancy unit of the cluster node.
[47]	An apparatus as claimed in claim 40, wherein the processor is configured to perform a switchover of a load allocation alternative inside the network element.

Huawei Technologies Co., Ltd. ("Huawei" or "Petitioner") petitions for *Inter Partes* Review ("IPR") of claims 1-6, 8-12, 18-24, 40-45, and 47 ("the Challenged Claims") of U.S. Patent 7,423,962 ("the '962 patent").

I. MANDATORY NOTICES—37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest—37 C.F.R. § 42.8(b)(1)

Huawei Technologies Co., Ltd.; Huawei Device USA, Inc.; Huawei Technologies USA Inc.; Huawei Investment & Holding Co., Ltd.; Huawei Device (Shenzhen) Co., Ltd.; Huawei Device Co., Ltd.; Huawei Tech. Investment Co., Ltd.; and Huawei Device (Hong Kong) Co., Ltd. are the real parties-in-interest. No other parties had access to or control over this Petition, and no other parties funded this Petition.

B. Related Matters—37 C.F.R. § 42.8(b)(2)

WSOU Investments, LLC d/b/a Brazos Licensing and Development ("WSOU")—the alleged Patent Owner—filed a complaint against Huawei Technologies Co., Ltd. and Huawei Technologies USA Inc. asserting the '962 patent on September 29, 2020 in the U.S. District Court for the Western District of Texas (Case No. 6:20-cv-00917). The complaint was one of six patent lawsuits filed by WSOU against Huawei between September 29, 2020 and October 2, 2020:

Asserted Patent No.	Civil Case No. (W.D. Tex.)
6,704,304	6-20-cv-00889
7,406,260	6-20-cv-00891
7,460,658	6-20-cv-00892
7,933,211	6-20-cv-00893
7,406,074	6-20-cv-00916
7,423,962	6-20-cv-00917

None of the six asserted patents is related to another.

Petitioner is not aware of any disclaimers or reexamination certificates addressing the '962 Patent.

C. Lead And Back-Up Counsel—37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel.

Lead Counsel	Backup counsel
Michael T. Hawkins, Reg. No. 57,867 Fish & Richardson P.C. 3200 RBC Plaza 60 South Sixth Street Minneapolis, MN 55402 Tel: 612-337-2569 hawkins@fr.com	Kenneth Hoover, Reg. No. 68,116 Tel: 512-226-8117 / hoover@fr.com Kim Leung, Reg. No. 64,399 Tel: 858-6784713 / leung@fr.com Nicholas Stephens, Reg. No. 74,320 Tel: 612-766-2018 / nstephens@fr.com Sangki Park, Reg. No. 77,261 Tel: 612-638-5763 / spark@fr.com Rishi Gupta, Reg. No. 64,768 Tel: 214-292-4056 / rgupta@fr.com Patrick J. Bisenius, Reg. No. 63,893 Tel: 612-766-2048 / bisenius@fr.com Terry J. Stalford, Reg. No. 39,522 Tel: (214) 292-4088 / stalford@fr.com

D. Service Information

Please address all correspondence and service to the address listed above. Petitioner consents to electronic service by email at 35548-0133IP1@fr.com (referencing No. 35548-0133IP1 and cc'ing PTABInbound@fr.com and hawkins@fr.com).

II. PAYMENT OF FEES—37 C.F.R. § 42.103

Huawei authorizes the Office to charge Deposit Account No. 06-1050 for the fee set in 37 C.F.R. § 42.15(a) and further authorizes payment for any additional fees to be charged to this Deposit Account.

III. REQUIREMENTS FOR IPR—37 C.F.R. § 42.104

A. Standing—37 C.F.R. § 42.104(a)

Huawei certifies that the '962 patent is available for IPR and that Huawei is not estopped from requesting IPR.

B. The Challenge and Relief Requested—37 C.F.R. § 42.104(b)

Huawei requests IPR of claims 1-6, 8-12, 18-24, 40-45, and 47 of the '962 patent on the grounds listed below. A declaration from Dr. Nathaniel Davis (EX1003) supports this Petition.

Ground	Basis for Rejection
Ground 1	Claims 1-6, 8-12, 18-24, 40-45, and 47 are anticipated under 35 U.S.C. §102(e) by U.S. Patent No. 6,885,633 to ("Mikkonen"; EX1004)
Ground 2	Claims 1-6, 8-12, 18-24, 40-45, and 47 are rendered obvious

Ground	Basis for Rejection
	under 35 U.S.C. §103 by Mikkonen in view of VIRTUAL ROUTER REDUNDANCY PROTOCOL ("RFC 2338"; EX1005)

The '962 patent was filed on June 19, 2003 as PCT application PCT/FI03/00507 which claims priority to Finnish application FI20021287, filed on June 28, 2002. Application PCT/FI03/00507 entered the National Stage in the United States on February 20, 2004. This Petition treats June 28, 2002 as the Critical Date for evaluating prior art status:

Reference	Filing/Priority	Publication	Status
Mikkonen (EX1004)	Apr. 10, 2000	Apr. 26, 2005	§ 102(e)
RFC 2338 (EX1005)	N/A	April 1998	§ 102(b)

Mikkonen is a published U.S. patent filed on April 10, 2000—years before the Critical Date. EX1004, 1. Regarding RFC 2338, the evidence here confirms that it was an IETF publication known to interested members of the public and publicly accessible no later than April 1998. EX1007, ¶11. Neither reference was cited during examination.

IV. THE '962 PATENT

A. Brief Description

The '962 patent relates to processes, systems, and apparatus to provide "redundancy" and "load balancing in telecommunication systems" such as "packet-switched mobile system." EX1001, 1:6-10; *see also* 1:58-62, 2:17. The patent employs pairs of "cluster nodes" or "processing units" to serve as "backup units for each other." *Id*., 1:65-2:3. Each "cluster node" hosts one or more "logical nodes," which the '962 patent also refers to as "virtual nodes" or "virtual cluster nodes." *Id*., 2:3-4, 5:21-23. The "virtual nodes" hosted by different "cluster nodes" are grouped into redundancy pairs which the '962 patent refers to as "load allocation alternatives." *Id*., 5:21-49. In each pair, "one of the logical nodes is active and the other is on standby." *Id*., 2:8-9. The '962 patent purports to provide redundancy "based on the idea that when a [cluster] node malfunctions ... the standby logical node of the pair ... becomes the active logical node" and performs the functions of the active node. *Id*., 2:12-16. Each pair of virtual nodes, or "load allocation alternative" is associated with "an external IP address that is used as the user plane address." *Id*., 5:54-55.

B. Prosecution History

In the last office action, the examiner rejected each of the independent claims as anticipated by Rathunde (US 6,574,477). EX1002, 54-61. The examiner also indicated that several dependent claims would be allowable if written into independent form because they each "recite[d] essentially the same limitation ... 'wherein also

an individual external routing address is defined for each load allocation alternative, on the bases of which data is transmitted to the network element.'" EX1002, 14-15 (underlining in original). The examiner further noted that this sole feature was not disclosed by the cited art. *Id.*

In response to the office action, the applicant amended each independent claim to include the limitation of an "individual external routing address" being defined "for each load allocation alternative." EX1002, 32-45. The applicant also included this limitation in a new independent claim (claim 44). *Id*. The examiner subsequently issued a notice of allowance indicating this sole limitation as the basis for the allowance. EX1002, 12-15; EX1003, ¶33.

As described below, more pertinent prior art publications never considered by the examiner disclosed this feature.

V. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art at the time of the '962 patent (a "POSITA") would have had a Master's degree in computer science, computer engineering, or a related field, with 3-5 years of experience in data communication networks. EX1003, ¶¶27-31. Such expertise could be obtained through research and study in a graduate program or through comparable exposure to research literature through industry employment working in the field of network management. *Id*. Additional years of experience could substitute for the advanced degree. *Id*.

VI. CLAIM CONSTRUCTION

All claim terms should be construed according to the *Phillips* standard. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. §42.100. In the Related Litigation, a *Markman* hearing is scheduled for August 12, 2021. EX1101, 3. Given the noticeable similarity between the predictable combination in Grounds 1-2 (below) and the preferred embodiment of the '962 patent, no construction is necessary. *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011).

VII. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. GROUND-1: Mikkonen anticipates claims 1-6, 8-12, 18-24, 40-45, and 47.

1. Mikkonen

Similar to the '962 patent, Mikkonen relates to "providing fault tolerance in computer data networks." EX1004, 1:6-7. Mikkonen describes a "fault tolerant" network device that employs two internal network nodes. *Id.*, 1:62-66. In Mikkonen, "fault tolerance is achieved by redundancy, i.e. by using [the] at least two network nodes in parallel." *Id.*, 2:14-16. Furthermore, Mikkonen assigns individual network addresses to each pair of network nodes. Mikkonen explains that "[a] first network interfaces [*sic*] on the first node has the same IP and MAC address as one interface on the second node, and the second network interface on the first node has the same IP and MAC address as the other interface on the second node." *Id.*, 2:20-24. Mikkonen describes that during "normal operations" of the fault tolerant unit "a

first node of the two nodes handles traffic directed to the first IP address and ignores the traffic directed to the second IP address, and the second node handles traffic directed to the second IP address and ignores the traffic directed to the first IP address." *Id*., 2:33-37. Then, the "two nodes monitor each other for fault conditions" so that if a fault occurs "the other node activates the other of its interfaces and starts handling traffic directed to both IP addresses." *Id*., 2:37-41.

Furthermore, Mikkonen seeks to improve upon previously existing redundancy protocols, "namely RFC 2281 'Cisco Hot Standby Router Protocol' (HSRP) and RFC 2338 'Virtual Router Redundancy Protocol' (VRRP)." *Id*., 1:21-26, 1:58-62. Specifically, Mikkonen notes that these protocols can be "complicated and generate some, signaling traffic overhead." *Id*., 1:48-50. Thus, Mikkonen aims to provide a "structure for a fault tolerant system which is simple in construction, and does not create traffic overhead in the network." *Id*., 1:60-62.

For these reasons and as further detailed in the element-by-element analysis below, claims 1-6, 8-12, 18-24, 40-45, and 47 are anticipated by Mikkonen.

2. Analysis

(a) Claim 1

Element [1.P]

To the extent the preamble is limiting, Mikkonen discloses this element. EX1003, ¶59. Mikkonen describes a "fault tolerant unit" that employs at least two

"network nodes" to execute network redundancy and load allocation processes that improve upon the "Hot Standby Router Protocol (HSRP)" and the "Virtual Router Redundancy Protocol (VRRP)." EX1004, 1:21-26, 1:58-59, 3:9-52 (explaining the general operations of the fault tolerant firewall unit 100). Thus, Mikkonen discloses a method of operation for the firewall unit 100.

Element [1.a]

Mikkonen discloses first and second physical cluster nodes that are configured to transmit data. EX1003, ¶60. For example, in one embodiment of Mikkonen's "network nodes," Mikkonen discloses a firewall unit 100 (e.g., the fault tolerant unit) that includes at least two firewall nodes 100a, 100b. Each firewall node 100a, 100b is a physical cluster node that includes "four physical network interfaces 110." EX1004, 3:2-4, FIG. 1.

Each firewall node 100a, 100b is capable of transmitting data. EX1003, ¶61. Mikkonen states that: "[i]n normal operation, *node 100a forwards traffic arriving from network 10 to IP address IPA via network interfaces 110a and 110c to the second network 20*, and traffic arriving from the second network 20 to IP address IPC via network interfaces 110c and 110a to the first network. ... Similarly, the second *node 100b forwards traffic arriving from network 10 to IP address IP B via network interfaces 110g and 110h to the second network 20*, and traffic arriving from the second network 20 to IP address IP D via network interfaces 110h and

110g to the first network." EX1004, 3:9-21.[1]

Each firewall node also serves as a redundancy unit to the other firewall node. EX1003, ¶62. Mikkonen explains that "[a]ccording to the invention, fault tolerance is achieved by redundancy, i.e. by using at least two network nodes in parallel." EX1004, 2:14-16. During normal operations, "a first node of the two nodes handles traffic directed to the first IP address and ignores the traffic directed to the second IP address, and the second node handles traffic directed to the second IP address and ignores the traffic directed to the first IP address." EX1004, 2:33-37. However, if a fault occurs in one of the nodes, the backup node begins handling traffic directed to the IP address of the previously active, but now faulty, node. EX1003, ¶62. Mikkonen explains that "The two nodes monitor each other for fault conditions, and if one of the nodes show signs of failure, the other node activates the other of its interfaces and starts handling traffic directed to both IP addresses. These two nodes form a fault tolerant unit, and more than one such units can be used in parallel for higher capacity." EX1004, 2:37-40.

Like VRRP and HSRP (which Mikkonen seeks to improve (*see* EX1004, 1:13-55)), Mikkonen's system employs two physical firewall nodes to host and backup a virtual node with its own specific IP address. EX1003, ¶63. For instance, Mikkonen explains that according to the VRRP protocol:

[1] All emphases added unless otherwise noted.

> One of the routers running the VRRP protocol acts as the master for a virtual router, i.e. performs the duties of the virtual router. The VRRP protocol provides a mechanism for transferring the duties to another router in the case of failure of the master router. Each virtual router has an IP address and a MAC address, which are used by hosts for transmission of data via the virtual router.

EX1004, 1:39-45.

As Mikkonen explains from the VRRP protocol, each virtual router is defined by a specific IP address, "which are used by hosts for transmission of data via the virtual router." EX1003, ¶64. When router is "virtual" the actual physical network node handling traffic directed to the IP address of the virtual router is transparent to the hosts. EX1003, ¶64. Thus, from the hosts' perspective, information sent to the "virtual router" e.g., the IP address of the virtual router, is processed by the virtual node without the hosts being aware of a malfunction of the active physical node. EX1003, ¶64.

Mikkonen's firewall nodes function in a manner similar to a router hosting a VRRP virtual node. EX1003, ¶65. Mikkonen defines "virtual" IP/MAC address combinations which are each hosted by one physical firewall node acting in the capacity of an active master of the IP/MAC address combination and by the other physical firewall node acting in a backup capacity for the IP/MAC address combination. EX1004, FIG. 1 (annotated below); EX1003, ¶65. Specifically, in Mikkonen's system each firewall node 100a/100b (i.e., cluster nodes) actively "handles

traffic directed to [one] IP address" and serves as a backup to the IP address for which the other firewall node is actively handling traffic. EX1004, 2:18-41, 3:9-11, 3:35-38, FIG. 1 (annotated below); EX1003, ¶65. For instance, "in normal operation, node 100a forwards traffic arriving from network 10 to IP address IP A via network interfaces 110a and 110c to the second network 20 ... if node 100b observes that node 100a has stopped functioning, node 100b activates the previously inactive interfaces 110e and 110f, and starts handling traffic directed to IP addresses IP A and IP C." EX1004, 3:9-11, 3:35-38; 4: 21-37 ("The inventive structure virtually eliminates outages caused by a fault in at hardware component ... [t]he system is able to detect a fault and transfer the functionality of the broken node to another node transparently, unnoticed by the user ..."). Furthermore, the fault in node 100a is transparent to host computers on the network. EX1004, 3:39-44 ("any network element ... need not know about the possible fault ..."); EX1003, ¶65.

In other words, as depicted in annotated FIG. 1, firewall node 100a acts as an active master for a virtual node with IP address A and a backup to a virtual node with IP Address B. EX1004, FIG. 1; EX1003, ¶66. Interface 110a serves as a physical network interface for the virtual node associated with IP address A and interface 110b serves as a physical network interface for the virtual node associated with IP address B. EX1004, FIG. 1; EX1003, ¶66. Likewise, firewall node 100b

acts as an active master for IP address B and a backup to IP address A. EX1004, FIG. 1; EX1003, ¶66. And, interface 110e serves as a network interface for the virtual node associated with IP address A and interface 110g serves as a network interface for the virtual node associated with IP address B. EX1004, FIG. 1; EX1003, ¶66.

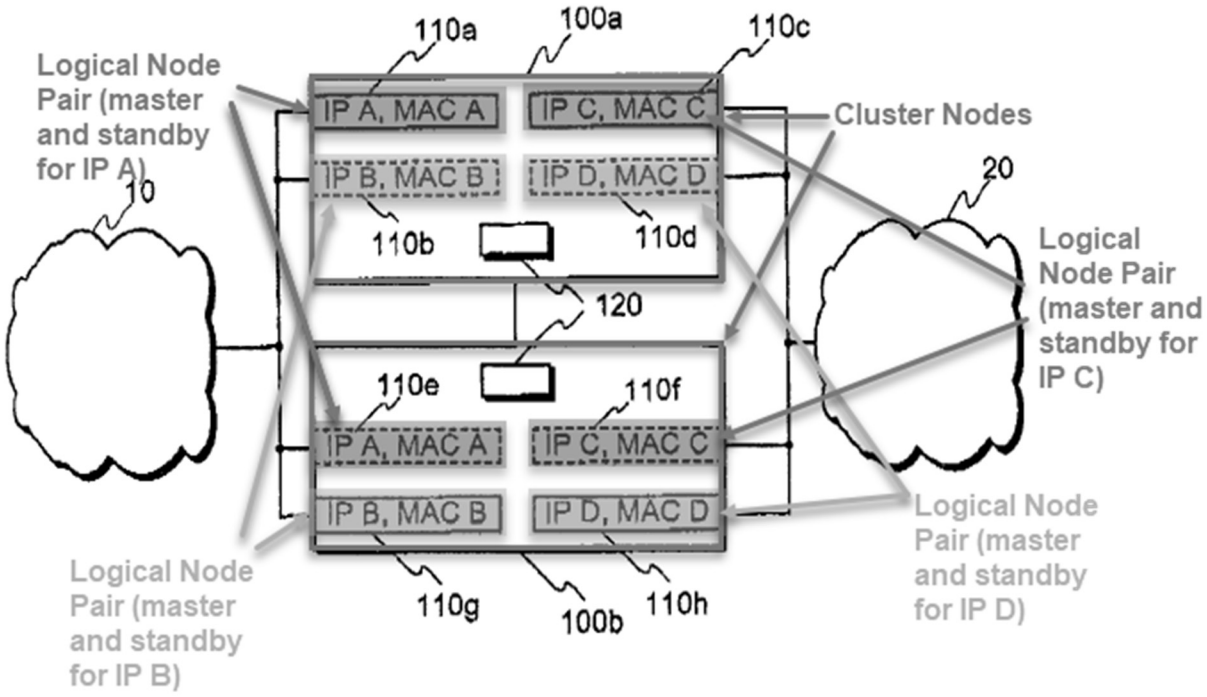


Fig. 1

EX1004, FIG. 1 (annotated).

A POSITA would have readily recognized from Mikkonen's teaching that the disclosed process employs the use of virtual firewall nodes (represented by the IP/MAC addresses) hosted by each of the two physical firewall nodes. EX1003, ¶67. For instance, Mikkonen's virtual firewall node uses the same address (e.g., IP

address IP A) when hosted as a virtual master node on firewall node 100a during normal operation or when hosted as a virtual backup node on firewall node 100b during backup operations (e.g., if node 100a malfunctions). EX1004, 2:18-41, 3:9-11, 3:35-38, FIG. 1. Consequently, Mikkonen discloses the use of virtual or logical nodes. EX1003, ¶67.

Finally, because, the '962 patent explains that the term "logical nodes" is a synonym for "virtual cluster nodes" or "virtual nodes," (EX1001, 5:21-23), Mikkonen's virtual firewall nodes hosted by the physical firewall nodes (e.g., cluster nodes) correspond to the logical nodes recited in claim 1.

Element [1.b]

Mikkonen discloses the formation of load allocation alternatives between logical nodes. EX1003, ¶70. The '962 patent explains load allocation alternatives as a "directed virtual node pair [that] has a feature visible outside the network element called a load allocation alternative LBX1, LBX2, LBY1, LBY2, LBZ1, LBZ2, which is a logical Gn, Gp or Gi interface ... Each load allocation alternative has an individual external user plane IP address at the Gn or Gp interface for receiving the data packets" EX1001, 5:30-33, 6:4-6, Table 1, FIG. 2 (annotated below).

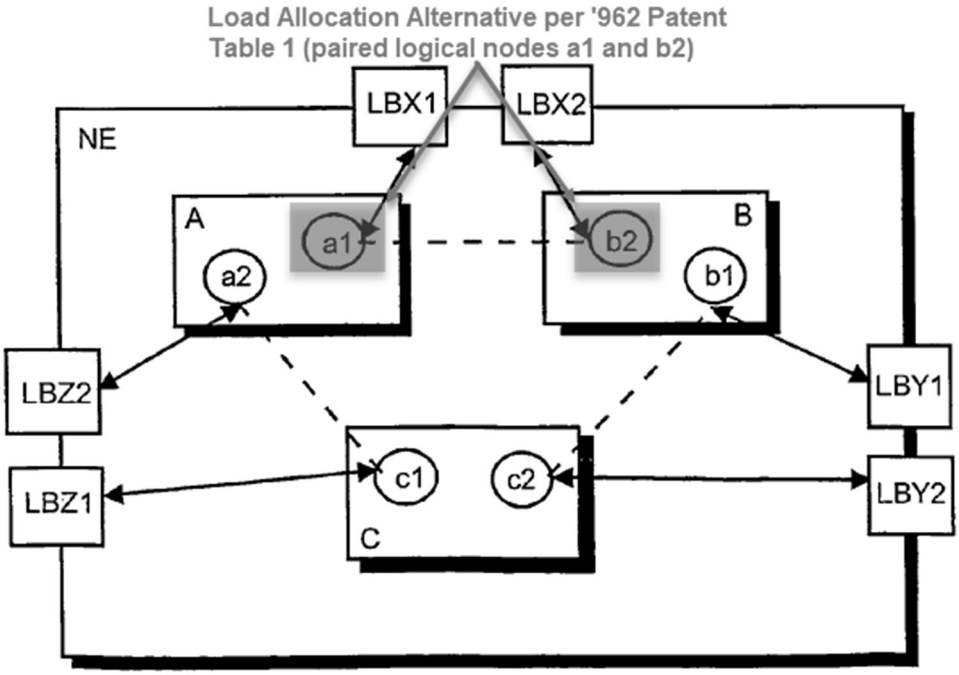


Figure 2

EX1001, FIG. 2 (annotated).

Mikkonen similarly pairs virtual nodes into load allocation groups with one each residing on different physical nodes 100a and 100b and each load allocation alternative being associated with a network interface and a single external IP address. *See* EX1004, FIG. 1 (annotated below), 3:9-44; EX1003, ¶71. Mikkonen pairs the virtual node associated with interface 110a together with the virtual node associated with interface 110e into a load allocation alternative using the single external IP address IP A, and pairs the virtual node associated with interface 110g together with the virtual node associated with interface 110b into a load allocation alternative using the single external IP address IP B. Mikkonen describes that "[i]n

normal operation, node 100a forwards traffic arriving from network 10 to IP address IP A via network interfaces 110a and 110c to the second network 20 ... if node 100b observes that node 100a has stopped functioning, node 100b activates the previously inactive interfaces 110e and 110f, and starts handling traffic directed to IP addresses IP A and IP C." EX1004, 3:9-11, 3:35-38. Together, the group of nodes associated with IP address A form one load allocation alternative and the group of nodes associated with IP address B form a second load allocation alternative, as described by the '962 patent. EX1003, ¶71.

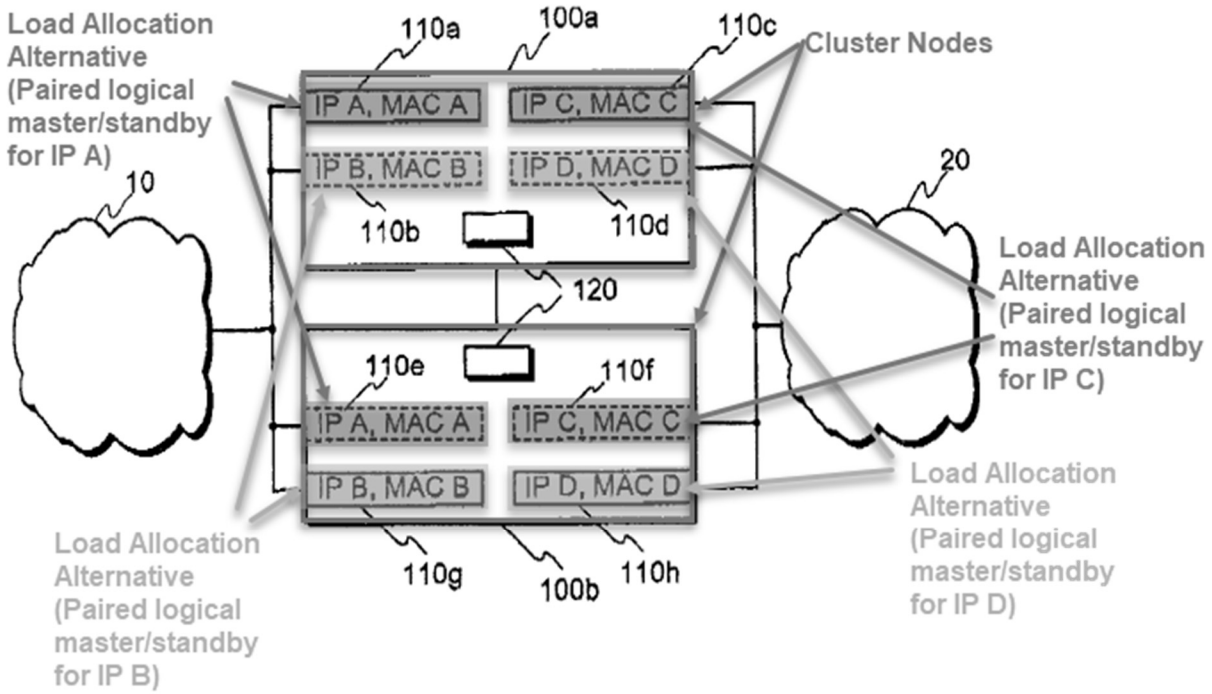


Fig. 1

EX1004, FIG. 1 (annotated).

Furthermore, FIG. 1 of Mikkonen illustrates that the virtual nodes associated

with each load allocation alternative are distributed between the two firewall nodes 100a/100b, with one residing on each firewall node. Using the load allocation alternative associated with IP address A as an example, firewall node 100a acts as the active master virtual node and firewall node 100b acts as the standby or backup node. EX1004, 3:9-11, 3:35-38; EX1003, ¶72.

What is more, like the '962 patent, Mikkonen splits, or allocates, the host loads of network 10 between two load allocation alternatives (e.g., one associated with IP address IP A and one associated with IP address IP B) for load balancing. EX1003, ¶73. "For load balancing reasons, it is advantageous that half of the hosts in network 10 are configured to use IP address IP A for traffic directed to the second network 20, and the second half to use IP address IP B for traffic directed to the second network 20." EX1004, 3:45-49; *see also* EX1001, 6:13-15.

Element [1.c]

Mikkonen discloses performing a switchover of nodes within a load allocation alternative when one of the active nodes malfunctions. EX1003, ¶75. Mikkonen discloses that each firewall node monitors the other for malfunctions. "Nodes 100a and 100b have a communication link between them in order to allow monitoring and testing of each other." EX1004, 3:30-33. If one firewall node malfunctions, the other firewall node executes a switchover and begins managing traffic directed to the IP address(es) of the virtual nodes associated with the malfunctioning firewall

node. EX1003, ¶75. For instance, Mikkonen explains that "[i]f node 100a observes that node 100b has stopped functioning, *node 100a activates the previously inactive interfaces 110b and 110d, and starts handling traffic directed to IP addresses IP B and IP D*." EX1004, 3:33-35, see also FIG. 1 (annotated below); EX1003, ¶75.

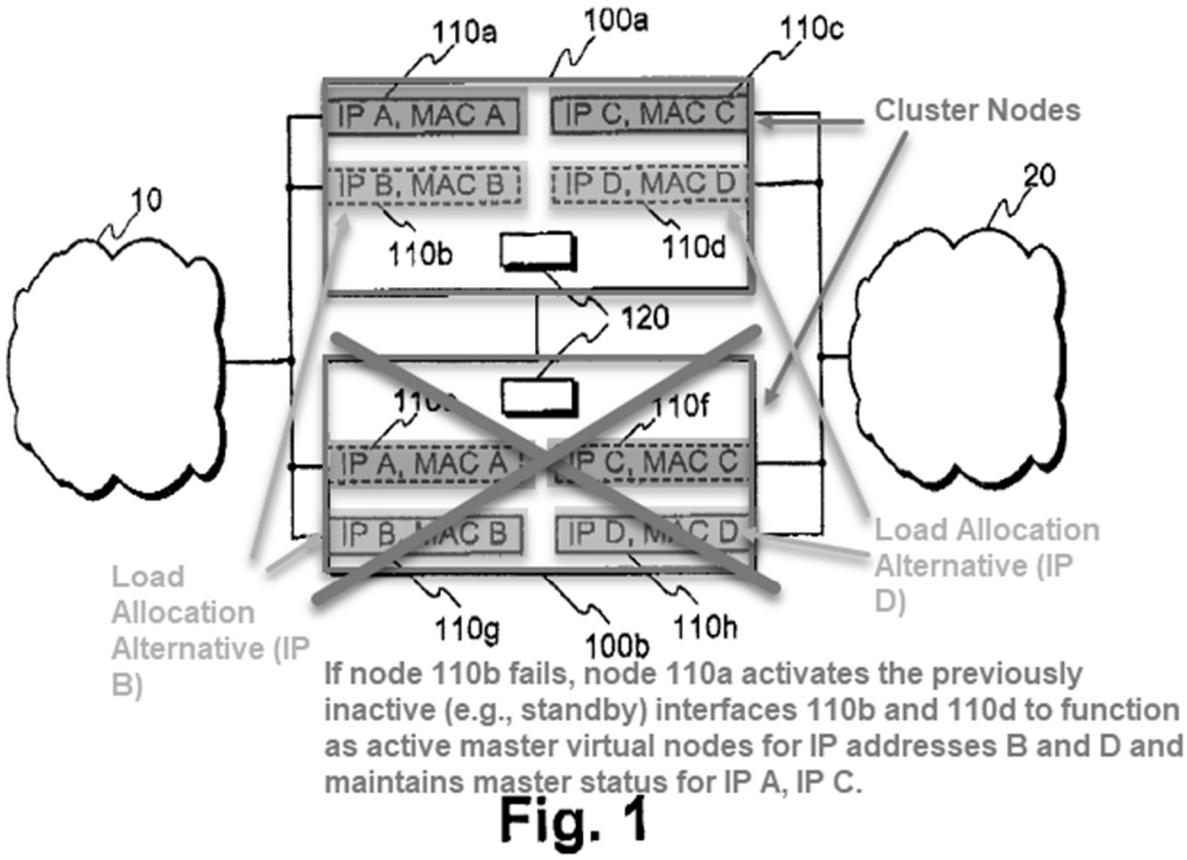


Fig. 1

EX1004, FIG. 1 (annotated).

The previous standby virtual node associated with the respective IP addresses B and D is switched into an active status by the activation of previously inactive interfaces 110b and 110d of firewall node 100a to actively handle the traffic directed to IP addresses B and D, respectively. EX1003, ¶76. By extension, the

previously active virtual node of firewall node 100b is no-longer active by virtue of the malfunction, and it can be considered to be in standby until it is repaired and can resume an active status. EX1003, ¶76. In other words, the POSITA would have understood that when a transition of the backup node from standby to active occurs, the reverse operation occurs for the master- i.e., shifting from active to standby. EX1003, ¶76.

Element [1.d]

Mikkonen discloses that a network element comprises both firewall nodes 100a and 100b. EX1003, ¶78. In reference to FIGs. 1 and 2, Mikkonen explains that a single "firewall unit comprises two firewall nodes 100a, 100b." EX1004, 3:2-3. Mikkonen also states that these "two nodes form a fault tolerant unit, and more than one such units can be used in parallel for higher capacity." EX1004, 1:63-66; 2:41-43; FIG. 1 (annotated below).

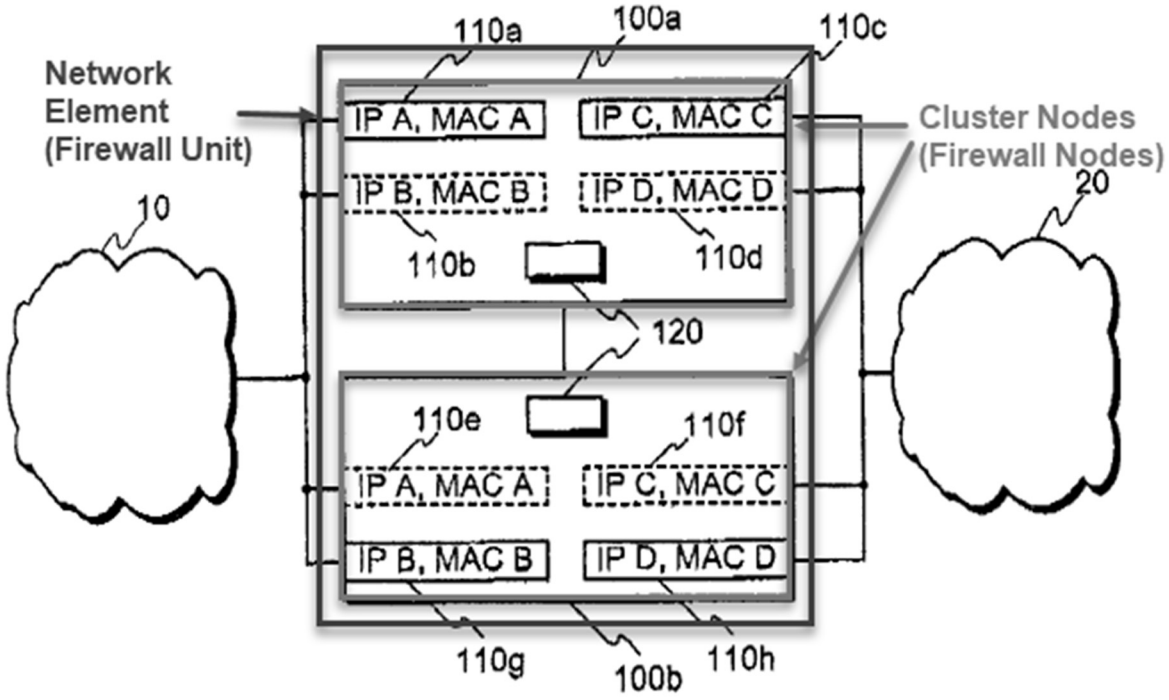


Fig. 1

EX1004, FIG. 1 (annotated).

Moreover, in FIG. 2, Mikkonen specifically outlines the firewall unit 200 "comprising two network nodes 100." EX1004 4:7-8, FIG. 2 (annotated below).

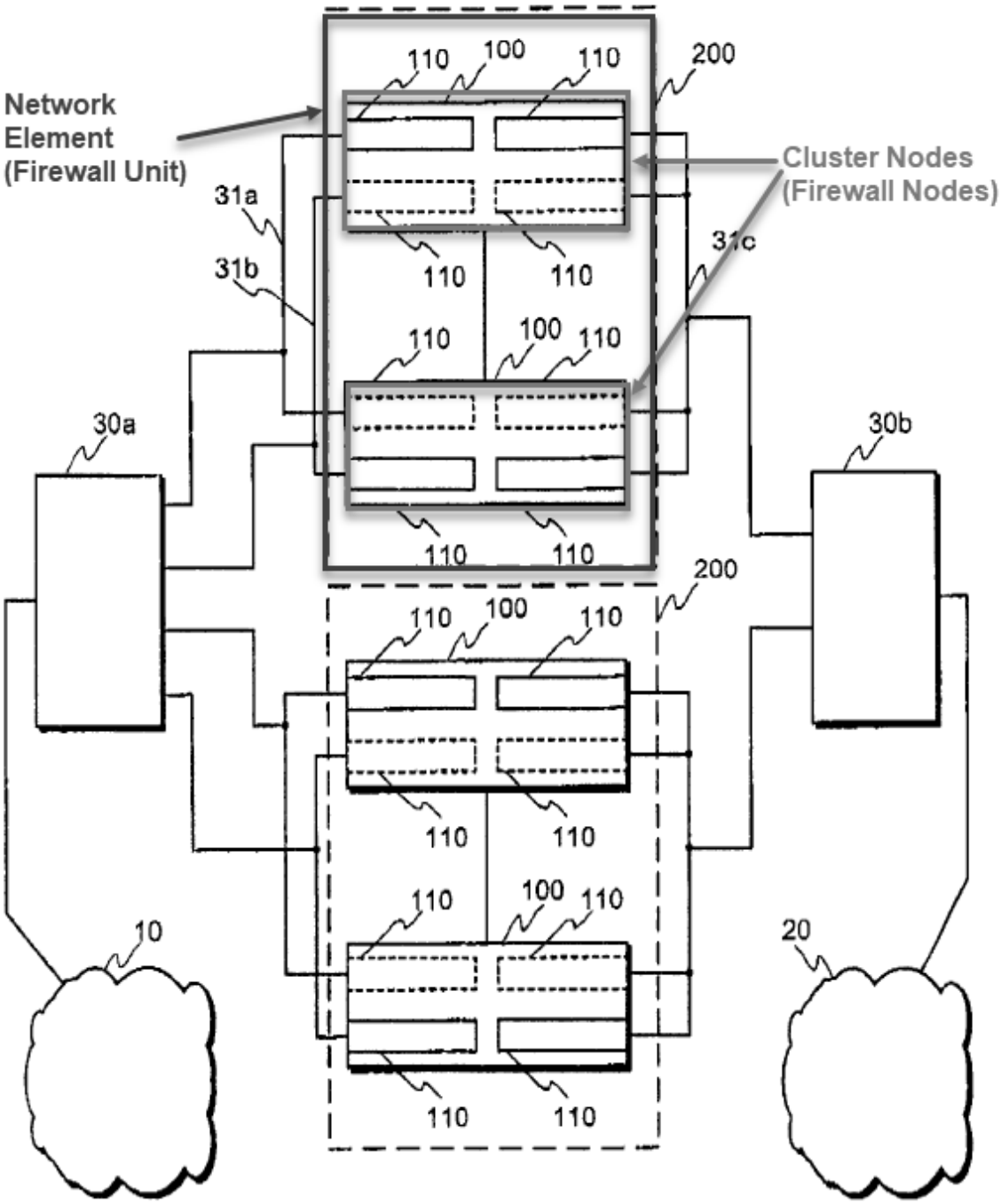


Fig. 2

EX1004, FIG. 2 (annotated).

Mikkonen also explains that the firewall nodes provide redundancy for the

firewall unit. EX1003, ¶80. Within the firewall unit the "two nodes typically provide enough redundancy, whereby the use of more than two nodes might not be necessary in many applications of the inventive structure." EX1004, 2:44-51. And Mikkonen explains that the redundancy and "[f]ault tolerant operation is provided by each of the two nodes of each [firewall] unit backing up the other node." EX1004, 4:10-12. Hence, the firewall unit is backed-up because the two nodes therein provide redundancy to each other. EX1003, ¶80.

Element [1.e]

Mikkonen discloses that an individual external routing address is defined for each load allocation alternative. EX1003, ¶82. In FIG. 1 (annotated below), Mikkonen demonstrates that unique IP/MAC address combinations are defined for each pair of virtual master and standby nodes. EX1004, 2:20-22 ("A first network interfaces on the first node has the same IP and MAC address as one interface on the Second node"). For example, the load allocation alternative formed using interface 110a of node 100a and interface 110e of node 100b is assigned IP address IP A. EX1004, 3:9-11; EX1003, ¶82. Likewise, the load allocation alternative formed using interface 110b of node 100a and interface 110g of node 100b is assigned IP address IP B. EX1004, 3:35-38; EX1003, ¶82.

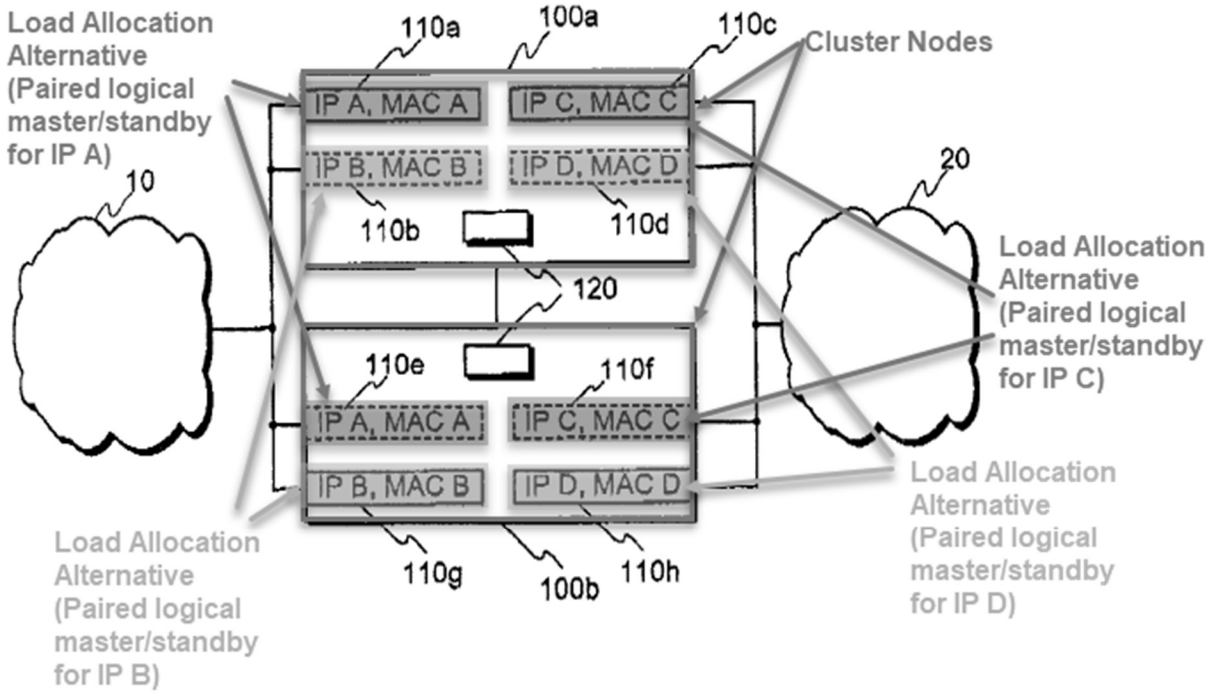


Fig. 1

EX1004, FIG. 1 (annotated).

Furthermore, Mikkonen states that these addresses (IP A and IP B) are used as the basis for which other nodes transmit data to the firewall nodes. EX1003, ¶83. Mikkonen explains that network "traffic arriving from network 10" at node 100a is addressed "to IP address IPA." EX1004, 3:9-11. Node 100a then forwards the traffic "via network interfaces 110a and 110c to the second network 20." *Id.* Additionally, Mikkonen explains that the common IP address for each load allocation alternative, "it is advantageous to connect interfaces with the same IP and MAC addresses to the same network segment, whereby *any network element in networks 10 and 20 need not know about the possible fault situation in one of the*

nodes and the corresponding change of flow of traffic." EX1004, 3:39-44, *see also* Abstract, 3:30-53; EX1003, ¶83. In other words, the key claim limitation that resulted in the allowance of the '962 patent was a well-known technique to make a network fault transparent to downstream hosts. EX1003, ¶83.

(b) Claim 2

Element [2]

Mikkonen discloses that traffic in the network is distributed between firewall nodes 100a/100b. EX1003, ¶85. Mikkonen splits the host loads of network 10 between IP address IP A and IP address IP B for load balancing. EX1003, ¶85. For instance, Mikkonen explains that "[f]or load balancing reasons, it is advantageous that half of the hosts in network 10 are configured to use IP address IP A for traffic directed to the second network 20, and the Second half to use IP address IPB for traffic directed to the Second network 20." EX1004, 3:45-49. As explained previously, node 100a operates as the active master virtual node for IP address IP A and node 100b operates as the active master virtual node for IP address IP B. EX1004, 3:9-29; EX1003, ¶85. Accordingly, in Mikkonen, the network traffic is distributed between firewall nodes 100a/100b. EX1003, ¶85.

(c) Claim 3

Element [3]

Mikkonen discloses that traffic in the network is distributed between firewall

nodes 100a/100b, each of which host a virtual node. EX1003, ¶87. Mikkonen splits the host loads of network 10 between IP address IP A and IP address IP B for load balancingEX1003, ¶87. For instance, Mikkonen explains that "[f]or load balancing reasons, it is advantageous that half of the hosts in network 10 are configured to use IP address IP A for traffic directed to the second network 20, and the Second half to use IP address IPB for traffic directed to the Second network 20." EX1004, 3:45-49. As explained previously, node 100a operates as the active master virtual node for IP address IP A and node 100b operates as the active master virtual node for IP address IP B. EX1004, 3:9-29; EX1003, ¶87. Accordingly, in Mikkonen, the network traffic is distributed between firewall nodes 100a/100b. EX1003, ¶87.

(d) Claim 4

Element [4]

Mikkonen discloses that traffic in the network is distributed between firewall nodes 100a/100b according to a specific load allocation plan. EX1003, ¶89. Mikkonen splits the host loads of network 10 between IP address IP A and IP address IP B for load balancing, by configuring "half of the hosts in network 10 [] to use IP address IP A ... and the second half to use IP address IP B." EX1004, 3:45-49; EX1003, ¶89.

(e) Claim 5

Element [5.a]

Mikkonen discloses that information is maintained on the two firewall nodes associated with the load allocation alternative. EX1003, ¶91. Mikkonen teaches that the firewall nodes 100a, 100b communicate with each other to monitor for malfunctions in the master node of each load allocation alternative. EX1004, 3:30-44; EX1003, ¶91. For example, Mikkonen's firewall nodes 100a/100b "have a communication link between them in order to allow monitoring and testing of each other." EX1004, 3:30-32. The communication link allows each firewall node to detect if the other node stops functioning. "If node 100a observes that node 100b has stopped functioning, node 100a activates the previously inactive interfaces 110b and 110d, and starts handling traffic directed to IP addresses IP B and IP D." EX1004, 32-35.

Similar to how the "standby unit" of the '962 patent "receives information on a malfunction of [an] interface used by the active unit" (EX1001, 7:3-6), Mikkonen's nodes 100a, 100b each gather and maintain testing information from the other node using a software module executed by the node processor. EX1003, ¶92. FIG. 1 (annotated below) "shows means 120 for observing the operation of another network node and for producing an indication about the operational state of said another network node." EX1004, 3:53-55. Each node "can perform tests on the node itself and report the results to the other node, and monitor the functioning of the other node." EX1004, 3:58-60.

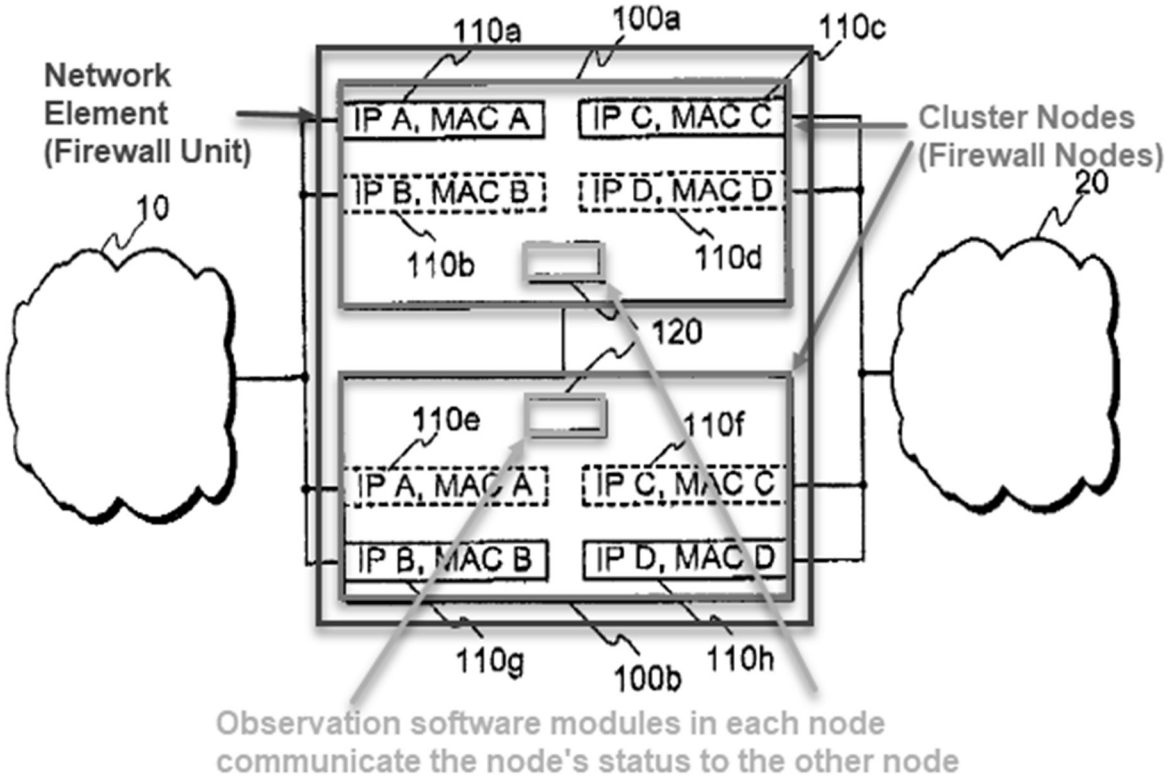


Fig. 1

EX1004, FIG. 1 (annotated)

Additionally, Mikkonen's firewall nodes 100a/100b must each maintain information related to filtering or blocking traffic because they can each "perform any filtering or blocking of traffic according to the tasks of a firewall node." EX1004, 3:25-27; EX1003, ¶93. Mikkonen does not explain this functionality in detail simply because it "is well known to a man skilled in the art." EX1004, 3:27-28; EX1003, ¶93. However, the POSITA would have understood that a firewall node must inherently store information such as lists of domain names and/or IP ad-

dresses of data to be filtered or blocked in order to perform the filtering and blocking operations of a firewall. EX1003, ¶93.

As yet another example, if Mikkonen's network nodes are implemented as routers rather than firewall nodes – as proposed in the summary of Mikkonen's invention (EX1004, 2:28-29 ("a network node such as a plain router or a firewall node")) – the router nodes must inherently maintain information such as routing tables in order to properly route data within a network. EX1003, ¶94. Such would have been similar to the "[f]orwarding information" maintained by the '962 patent's cluster nodes. EX1001, 6:50-57; EX1003, ¶94.

Element [5.b]

Mikkonen discloses that after a switchover data that was transmitted to the primary cluster node is then transmitted to the secondary cluster node. EX1003, ¶96. Mikkonen discloses that, before a switchover, data for IP address IP A is sent to node 100a and "node 100a forwards traffic arriving from network 10 to IP address IP A ... to the second network 20. EX1004, 3:9-10; EX1003, ¶96. Then, after a switchover the standby node – node 100b for IP addresses A and C, takes over managing traffic directed to those addresses. EX1003, ¶96. "[I]f node 100b observes that node 100a has stopped functioning, node 100b activates the previously inactive interfaces 110e and 110f, and starts handling traffic directed to IP addresses IPA and IP C." EX1004, 3:35-39.

(f) Claim 6

Element [6]

Claim 1 states that the "the first cluster node is a redundancy unit to the second cluster node and vice versa." So, in claim 6 "the redundancy unit" recited in claim 6 is understood to refer back to that recited in claim 1. Therefore, the second cluster node is the redundancy unit to the first cluster node. So, the "physical interface of the backup cluster node" would be a physical interface of the node serving as the redundancy unit to the active node that malfunctioned. In this regard, Mikkonen discloses this element. EX1003, ¶98. For instance, Mikkonen teaches that when one firewall node (e.g., node 100a) malfunctions the physical interfaces 110 of the other firewall node (e.g., node 100b) are activated and begin managing network traffic directed to the specific IP addresses of the load allocation alternative (e.g., IP addresses A and C). EX1004, 3:35-39 ("[I]f node 100b observes that node 100a has stopped functioning, node 100b activates the previously inactive interfaces 110e and 110f, and starts handling traffic directed to IP addresses IPA and IP C."); EX1003, ¶98.

(g) Claim 8

Element [8]

Mikkonen discloses this element. EX1003, ¶100. Mikkonen discloses that

the firewall nodes function using processors to execute functions via "software modules." EX1004, 3:56-57; EX1003, ¶100. Further, it is inherent that computer systems, such as network nodes, necessarily employed computer code to execute algorithms for computing network routes. *See e.g.,* EX1006, 13:25-34 (corroborating the ubiquitously known fact that computers functioned by executing code stored on computer readable media); EX1003, ¶100. Furthermore, it is also inherent that virtual nodes are software constructs, i.e., they are not specific hardware elements. EX1003, ¶100. And as discussed above (*supra*, Element [1a]) the process Mikkonen describes mirrors the virtual nodes used in VRRP protocols for a firewall by effectively forming virtual firewall nodes hosted by each of the two physical firewall nodes. EX1003, ¶100. Therefore, Mikkonen's virtual firewall nodes are inherently software-associated components of each physical node, i.e., they are necessarily defined by software rather than in physical hardware. EX1003, ¶¶100.

(h) Claim 9

Element [9.P]

To the extent the preamble is limiting, Mikkonen discloses this element. EX1003, ¶59. For example, Mikkonen describes the firewall unit that comprises [the] two firewall nodes 100a, 100b" as operating in a computer network in which "each node 100a, 100b [is] connected to [a] first network 10, and .. to [a] second network 20." EX1004, 2:67-3:8; FIG. 1.

Element [9.a]

Mikkonen discloses that both firewall nodes 100a/100b are comprised within a firewall unit. *Supra*, Ground-1 Element [1.d]; EX1003, ¶¶78-81.

Mikkonen also discloses that each firewall node 100a, 100b is capable of transmitting data and that each firewall node serves as a redundancy unit to the other firewall unit. *Supra*, Ground-1 Element [1.a]; EX1003, ¶¶61-69.

Element [9.b]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Element [1.a]; EX1003, ¶¶61-69.

Element [9.c]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Element [1.b]; EX1003, ¶¶70-74.

Element [9.d]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Element [1.c]; EX1003, ¶¶75-77.

Element [9.e]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Element [1.e]; EX1003, ¶¶82-84.

(i) Claim 10

Element [10]

Mikkonen discloses this element for the reasons detailed above. *Supra*,

Ground-1 Element [2]; EX1003, ¶¶85-86.

(j) Claim 11

Element [11.a]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Element [5.a]; EX1003, ¶¶91-95.

Element [11.b]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Element [5.b]; EX1003, ¶¶96-97.

(k) Claim 12

Element [12]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Element [6]; EX1003, ¶¶98-99.

(l) Claim 18

Element [18.P]

To the extent the preamble is limiting, Mikkonen discloses this element. EX1003, ¶102. For example, Mikkonen describes the firewall unit that "comprises [the] two firewall nodes 100a, 100b." EX1004, 2:67-3:8; FIG. 1.

Element [18.a]

Mikkonen discloses this element. EX1003, ¶¶103-104. Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Element [1.a]. Mik-

konen also discloses that the firewall nodes include processors, memory, and software to execute their assigned functions. EX1004, 3:56-64 (the nodes have a processor and software modules), 4:38-50 (the nodes have software "i.e., [an] operating system" and memory); EX1003, ¶104. Further, it is inherent that computer systems, such as network nodes, necessarily employed computer code to execute algorithms for computing network routes. *See e.g.,* EX1006, 13:25-34 (corroborating the ubiquitously known fact that computers functioned by executing code stored on computer readable media); EX1003, ¶104. Therefore, the processors of Mikkonen's network nodes must inherently execute software routines stored in memory to perform the processes described in Mikkonen.

Element [18.b]

Mikkonen discloses this element and corresponding structure for the reasons detailed above. *Supra*, Ground-1 Elements [18.a], [1.b]; EX1003, ¶¶105-106.

Element [18.c]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [18.a], [1.c]; EX1003, ¶¶107-108.

Element [18.d]

Mikkonen discloses this element and corresponding structure for the reasons

detailed above. *Supra*, Ground-1 Elements [18.a], [1.e];[2] EX1003, ¶¶109-110.

(m) Claim 19

Element [19]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [18.a], [2]; EX1003, ¶¶111-112.

(n) Claim 20

Element [20]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [18.a], [3]; EX1003, ¶¶113-114.

(o) Claim 21

Element [21]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [18.a], [4]; EX1003, ¶¶115-116.

(p) Claim 22

Element [22.a]

[2] Huawei notes that the "network element" recited in this claim does not have proper antecedent basis. However, for purposes of analyzing the IPR grounds here, the use of the term "network element" in claim 18 is similar to the use in claim elements [1.d] and [9.a].

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [18.a], [5.a]; EX1003, ¶¶117-118.

Element [22.b]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [18.a], [5.b]; EX1003, ¶¶119-120.

(q) Claim 23

Element [23]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [18.a], [6]; EX1003, ¶¶121-122.

(r) Claim 24

Element [24]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [18.a], [1.c], [1.e]; EX1003, ¶¶123-124.

(s) Claim 40

Element [40.P]

To the extent the preamble is limiting, Mikkonen discloses this element. EX1003, ¶59. For example, Mikkonen describes the firewall unit that "comprises [the] two firewall nodes 100a, 100b." EX1004, 2:67-3:8; FIG. 1.

Element [40.a]

Mikkonen discloses that each of the firewall nodes includes a processor. EX1004, 3:56-57; EX1003, ¶104. Furthermore, it is inherent that computing devices

such as network nodes include processors to execute software code. *See e.g.,* EX1006, 13:25-34 (corroborating the ubiquitously known fact that computers functioned by executing code stored on computer readable media); EX1003, ¶104.

Element [40.b]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Element [1.a]; EX1003, ¶¶60-69.

Element [40.c]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Element [1.b]; EX1003, ¶¶70-74.

Element [40.d]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Element [1.c]; EX1003, ¶¶75-77.

Element [40.e]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Element [1.e];[3] EX1003, ¶¶82-84.

(t) Claim 41

Element [41]

[3] Huawei notes that the "network element" recited in this claim does not have proper antecedent basis. However, Huawei interprets use of the term "network element" in claim 18 to be similar to the use in claim elements [1.d] and [9.a].

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [2], [40.P]-[40.e]; EX1003, ¶¶85-86.

(u) Claim 42

Element [42]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [2], [40.P]-[40.e]; EX1003, ¶¶87-88.

(v) Claim 43

Element [43]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [2], [40.P]-[40.e]; EX1003, ¶¶89-90.

(w) Claim 44

Element [44.a]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [2], [40.P]-[40.e]; EX1003, ¶¶91-95.

Element [44.b]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [2], [40.P]-[40.e]; EX1003, ¶¶96-99.

(x) Claim 45

Element [45]

Mikkonen discloses this element for the reasons detailed above. *Supra*, Ground-1 Elements [2], [40.P]-[40.e]; EX1003, ¶¶85-86.

(y) Claim 47

Element [47]

Mikkonen discloses this element. EX1003, ¶¶100-101. Mikkonen describes that the firewall nodes (processors therein) perform a switchover inside the firewall unit if one of the firewall nodes malfunction. *See supra*, Ground-1 Elements [40.a], [1.c]; EX1003, ¶¶100-101.

B. GROUND-2: The Mikkonen-RFC 2338 combination renders obvious claims 1-6, 8-12, 18-24, 40-45, and 47.

1. RFC 2338

RFC 2338 is an Internet standards document that defines the Virtual Router Redundancy Protocol (VRRP). EX1005, 1. VRRP is a protocol "designed to eliminate the single point of failure inherent in the static default routed environment" by the use of virtual routers. *Id*., 3. A virtual router is defined as "[a]n abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and a set of associated IP address(es) across a common LAN." *Id*., 4.

2. The combination of Mikkonen and RFC 2338

As noted above, Mikkonen's teaching directly relates redundancy protocols, such as VRRP, by providing a "structure for a fault tolerant system which is simple in construction, and does not create traffic overhead in the network." EX1004, 1:60-

62. In part, Mikkonen accomplishes the reduced overhead through the direct communication of monitoring and testing data between firewall nodes. EX1004, 3:30-32; 3:53-4:4; 4:21-33; EX1003, ¶53. Because Mikkonen's solution explicitly employs (and improves upon) VRRP, it would have been obvious to a POSITA to implement Mikkonen's firewall nodes using known aspects of VRRP. EX1003, ¶53. Specifically, it would have been obvious to the POSITA to implement Mikkonen's redundancy protocols using "virtual nodes" as was conventional in the VRRP protocol. EX1003, ¶53.

Multiple reasons would have motivated the POSITA to implement aspects of VRRP as defined in RFC 2338 into Mikkonen's firewall nodes. EX1003, ¶54. **First**, Mikkonen seeks to design a "fault tolerant system" and explicitly refers to VRRP as a typical protocol used to achieve fault tolerance. EX1004, 1:13-59; EX1003, ¶54. Further, Mikkonen's stated purpose is to reduce complexities and signaling overhead of VRRP. EX1004, 1:58-62. Therefore, when attempting to implement Mikkonen's teaching, a POSITA would have been prompted to employ fundamental aspects of the very protocol (VRRP) on which Mikkonen's improvement operated. EX1003, ¶54.

Second, Mikkonen describes the firewall nodes as already performing functions of a VRRP router that hosts virtual router(s)—the firewall nodes manage traffic directed to an abstract IP address that is shared between the nodes, with one

firewall node acting as the active master for the IP address (e.g., node 100a for IP address A and C), and the other acting as a backup for the same IP address (e.g., node 100b for IP addresses A and C). EX1004, 2:18-41; 3:9-11, 3:35-38; EX1003, ¶55; *compare* EX1004 FIG. 1 (below) *with* EX1005, 9 (diagram-below).

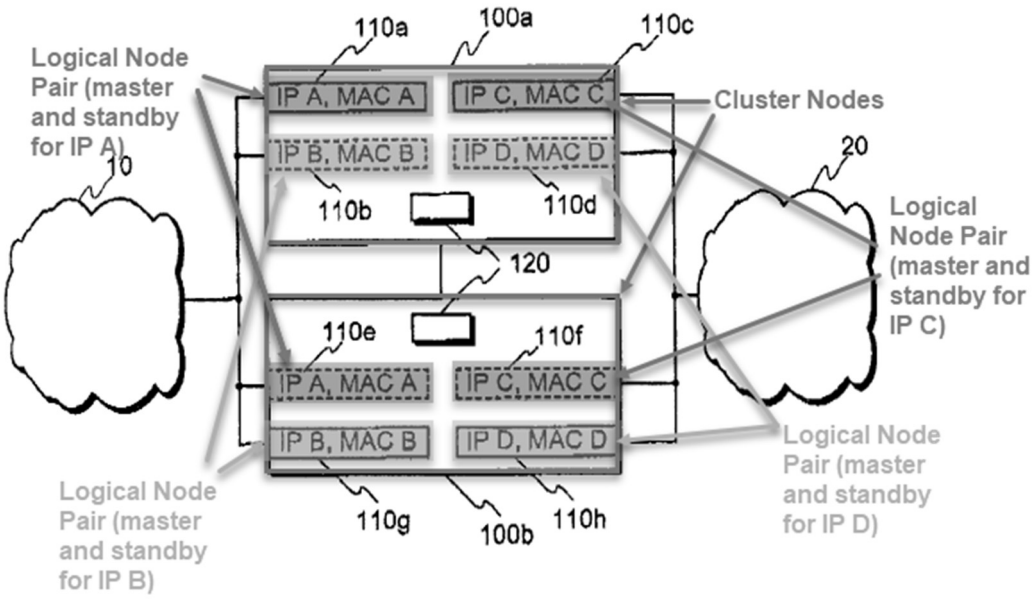
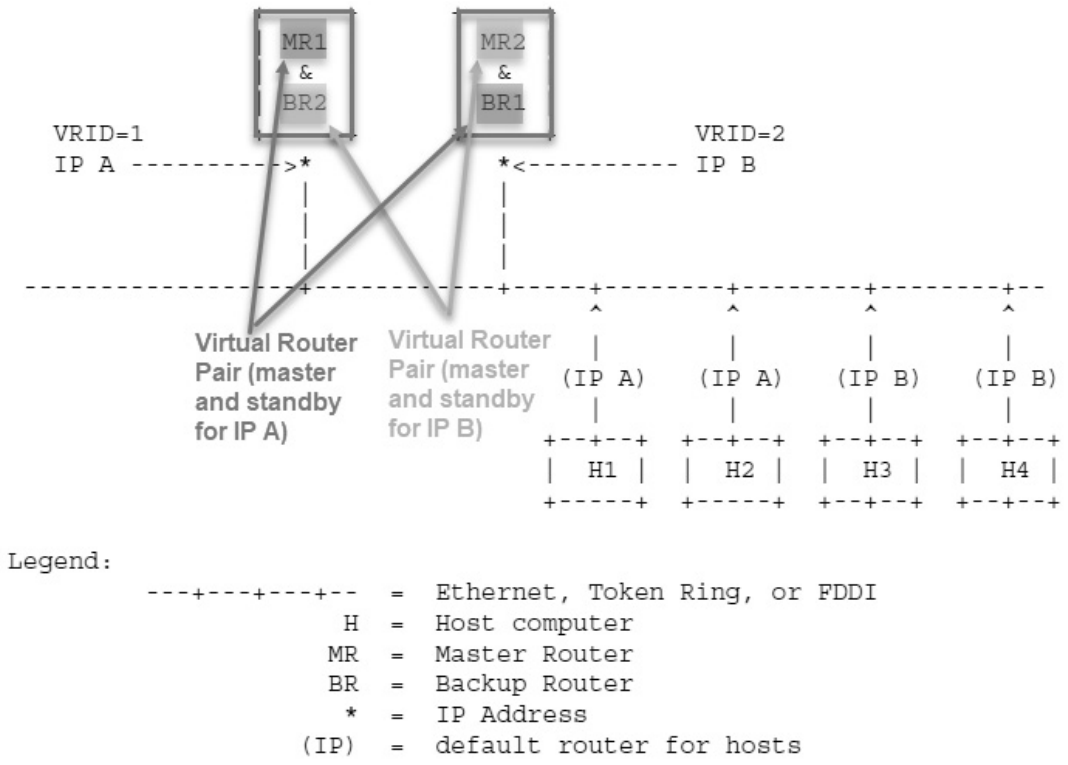


Fig. 1

EX1004, FIG. 1 (annotated)



EX1005, 9 (diagram-annotated)

Although Mikkonen's firewall nodes are described in a manner suggesting they host conventional "virtual nodes" in VRRP, Mikkonen does not expressly use the term "virtual nodes" or further describe a particular operations protocol for its firewall nodes. "[A] POSITA seeking to implement Mikkonen's fault tolerant system with direct monitoring communications between firewall nodes, would have been motivated to incorporate aspects the well-known VRRP protocols (such as virtual nodes) into Mikkonen's implementation." EX1003, ¶56. For instance, "[n]ot only would such a traditional solution have been recognized by a POSITA as a straightforward path to efficiently implement Mikkonen's fault tolerant system

using the VRRP protocol, but implementing virtual nodes as described in the VRRP protocol in Mikkonen's physical nodes would have been a routine task for the POSITA given the striking similarities in operation between Mikkonen's firewall nodes and the VRRP routers hosting virtual master and backup routers." EX1003, ¶56; EX1005, 4-5, 9 (Sample Configuration 2).

Third, a POSITA would have been prompted to implement Mikkonen's firewall nodes to host conventional "virtual nodes" of VRRP (as suggested in RFC 2338) due to the known benefits of adopting a well-known standard (VRRP) to minimize bugs/debugging delays and interoperability problems with existing systems. EX1003, ¶57. The example described in RFC 2338 is specific to routers in the VRRP protocol, but the evidence here confirms that a POSITA would have readily recognized why such virtual node concepts were applicable to firewall nodes. EX1003, ¶57; EX1004, 2:28-30). In fact, the POSITA would have understood that such routers were often configured to operate as firewall nodes at the time. EX1003, ¶57. Therefore, the POSITA would have had a reasonable expectation of success in modifying implementing Mikkonen's firewall nodes using such conventional "virtual nodes" of VRRP (as suggested in RFC 2338). EX1003, ¶57.

3. Analysis

(a) Claim 1

Element [1.P]

To the extent the preamble is limiting, Mikkonen discloses this element. *Supra*, Ground-1 Element [1.P]; EX1003, ¶125.

Element [1.a]

As previously described, Mikkonen discloses the claimed first and second cluster nodes configured to transmit data and serve as redundancy units to each other. *Supra*, Ground-1 Element [1.a].

To the extent the Board determines that Mikkonen does not teach the use of logical nodes, it would have been obvious for a POSITA to incorporate the fundamental concept of virtual nodes defined by the very protocol that Mikkonen seeks to improve into Mikkonen's firewall nodes. S*upra*, §VII.B.2; EX1003, ¶¶127, 53-54; *see also* EX1001, 5:21-23 (equating "virtual nodes" with "logical nodes"). For example, the RFC 2338 defines virtual routers as: "An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and a set of associated IP address(es) across a common LAN." EX1005, 4. Mikkonen describes the firewall nodes as managing traffic within a common network that is directed to a specific IP address shared between the firewall nodes, with one firewall node acting as the active master for the IP address (e.g., node 100a for IP address A and C), and the other acting as a backup for the same IP address (e.g., node 100b for IP addresses A and C). EX1004, 2:18-41; 3:9-11, 3:35-38; EX1003, ¶127. "This operation is similar to those of nodes that host a virtual

router master and backup according to VRRP." EX1003, ¶127; EX1005, 9. A virtual master is a "VRRP router that is assuming the responsibility of forwarding packets sent to the IP address(es) associated with the virtual router." EX1005, 4. A virtual backup is "the set of VRRP routers available to assume forwarding responsibility for a virtual router should the current Master fail." EX1005, 5.

Furthermore, the general operation of Mikkonen's firewall nodes 100a/100b and the physical interfaces 110a-110h would not be changed under the proposed combination with RFC 2338. EX1003, ¶128. As discussed above, the firewall nodes 100a/100b would still perform the same operations. EX1003, ¶128. Further, the interfaces 100a-100h would serve as physical interfaces for each virtual node hosted by the firewall nodes 100a/100b. EX1003, ¶128.

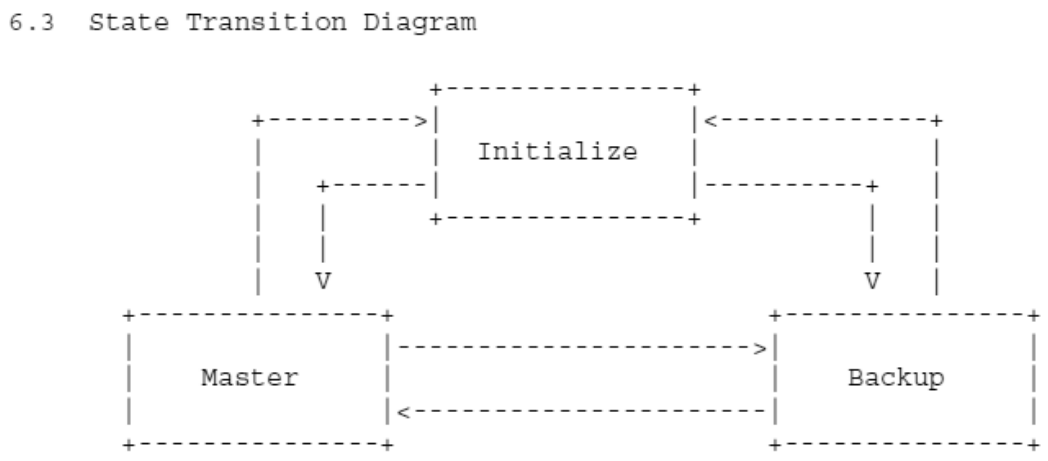
Consequently, because Mikkonen explicitly improves upon VRRP and the operations of Mikkonen's firewall nodes are already similar to those of VRRP router hosting virtual master and virtual backup routers in VRRP, it would have been obvious to a POSITA to incorporate the concept of virtual nodes from VRRP into Mikkonen's firewall nodes. S*upra*, §VII.B.2; EX1003, ¶129.

Element [1.b]

As previously described, Mikkonen discloses this element. *Supra*, Ground-1 Element [1.b].

Element [1.c]

As previously described, Mikkonen discloses this element. *Supra*, Ground-1 Element [1.c]. Additionally, in the Mikkonen-RFC 2338 combination, RFC 2338 corroborates the understanding that when a transition of a backup node from standby to active occurs, the reverse operation occurs for the master. EX1003, ¶132. When a master node malfunctions it reduces its priority from 255 to 0, indicating a shift to standby. EX1005, 11 ("The priority value for the VRRP router that owns the IP address(es) associated with the virtual router MUST be 255"), 17 ("If a shutdown event is received, then ... send an ADVERTISEMENT with priority = 0"). However, once repaired, the master node will re-assert itself as a master of because "a VRRP router will always become Master of any virtual router associated with the addresses it owns." EX1005, 7. For instance, once a malfunctioning master node is repaired and restarted it will enter the initialization state. EX1003, ¶132. During the initialization stage for a VRRP node "i]f the Priority = 255 (i.e., the router owns the IP address(es) associated with the virtual router)" the node is instructed to "[t]ransition to the {Master} state" and "send and ADVERTISEMENT." EX1005, 15, Section 6.3 Diagram (below); EX1003, ¶132. The backup node that took over master functions while during the master node's fault will receive the ADVERTISMENT with a Master Priority (255) and, in response, "[t]ransition back to the {Backup} state" for that virtual node/IP address. EX1005, 17-18; EX1003, ¶132.



EX, 1005, Section 6.3 Diagram.

Element [1.d]

As previously described, Mikkonen discloses this element. *Supra*, Ground-1 Element [1.d].

Element [1.e]

As previously described, Mikkonen discloses this element. *Supra*, Ground-1 Element [1.e].

(b) Claim 2

Element [2]

As previously described, Mikkonen discloses this element. *Supra*, Ground-1 Element [2].

(c) Claim 3

Element [3]

As previously described, Mikkonen discloses this element. *Supra*, Ground-1

Element [3].

(d) Claim 4

Element [4]

As previously described, Mikkonen discloses this element. *Supra*, Ground-1 Element [4].

(e) Claim 5

Element [5.a]

As previously described, Mikkonen discloses this element. *Supra*, Ground-1 Element [5.a].

Element [5.b]

As previously described, Mikkonen discloses this element. *Supra*, Ground-1 Element [5.b].

(f) Claim 6

Element [6]

As previously described, Mikkonen discloses this element. *Supra*, Ground-1 Element [6].

(g) Claim 8

Element [8]

As previously described, Mikkonen discloses this element. *Supra*, Ground-1 Element [8]. Additionally, in the Mikkonen-RFC 2338 combination, RFC 2338 defines a virtual node as "an abstract object" managed by a VRRP router. EX1005, 4.

An abstract object cannot be a physical hardware unit, but must be defined and implemented as a software-associated component. EX1003, ¶148.

(h) Claim 9

Element [9.P]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-1 Element [9.P].

Element [9.a]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Elements [1.a], [1.d]; Ground-1 Element [9.a].

Element [9.b]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [1.a].

Element [9.c]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [1.b].

Element [9.d]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [1.c].

Element [9.e]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [1.e].

(i) Claim 10

Element [10]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [2].

(j) Claim 11

Element [11.a]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [5.a].

Element [11.b]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [5.b].

(k) Claim 12

Element [12]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [6].

(l) Claim 18

Element [18.P]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-1 Element [18.P].

Element [18.a]

The Mikkonen-RFC2338 combination discloses this element. *Supra*,

Ground-2 Element [1.a]; Ground-1 Element [18.a].

Element [18.b]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Elements [1.b], [18.a].

Element [18.c]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Elements [1.c], [18.a].

Element [18.d]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Elements [1.e], [18.a]; Ground-1 Element [18.d].

(m) Claim 19

Element [19]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Elements [2], [18.a].

(n) Claim 20

Element [20]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Elements [3], [18.a].

(o) Claim 21

Element [21]

The Mikkonen-RFC2338 combination discloses this element. *Supra*,

Ground-2 Elements [4], [18.a].

(p) Claim 22

Element [22.a]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [5.a].

Element [22.b]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Elements [5.b].

(q) Claim 23

Element [23]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Elements [6], [18.a].

(r) Claim 24

Element [24]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-1 Element [24].

(s) Claim 40

Element [40.P]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-1 Element [40.P].

Element [40.a]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-1 Element [40.a].

Element [40.b]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [1.a].

Element [40.c]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [1.b].

Element [40.d]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [1.c].

Element [40.e]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [1.e]; Ground-1 Element [40.e].

(t) Claim 41

Element [41]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Elements [2].

(u) Claim 42

Element [42]

The Mikkonen-RFC2338 combination discloses this element. *Supra*,

Ground-2 Elements [3].

(v) Claim 43

Element [43]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Elements [4].

(w) Claim 44

Element [44.a]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Element [5.a].

Element [44.b]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Elements [5.b].

(x) Claim 45

Element [45]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-2 Elements [6].

(y) Claim 47

Element [47]

The Mikkonen-RFC2338 combination discloses this element. *Supra*, Ground-1 Elements [47].

VIII. INSTITUTION SHOULD NOT BE DISCRETIONARILY DENIED

In *Apple Inc. v. Fintiv, Inc.*, the Board enumerated six factors that provide a "holistic view" as to "whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in [a] parallel proceeding." IPR2020-00019, Paper 11 at 2-3 (PTAB "precedential" Mar. 20, 2020) ("*Fintiv I*"). Guided by precedent, Huawei took affirmative steps to promote the Board's efficiency and fairness goals. Huawei initiated this proceeding with exceptional diligence filing a single petition narrowly focused on specific claims within a mere nine weeks of learning of WSOU's asserted claims, and provided a stipulation akin to *Sand Revolution* to eliminate overlapping prior art grounds between the instituted IPR proceeding and the Related Litigation. EX1102, 1. Moreover, the actual trial date scheduled for the '962 patent is subject to speculation (because the '962 patent will be grouped into a jury trial for the "first of the consolidated cases" starting on September 26, 2022 or a later trial for the "remaining consolidated cases" on a subsequent (unknown) date). EX1101, 5. These facts, paired with the strong merits of Grounds 1-2, provide compelling reasons to institute. *Sand Revolution II, LLC v. Continental Intermodal Group*, IPR2019-01393, Paper 24, 12 (PTAB "Informative" June 16, 2020).

Relevant Facts—Between September 29, 2020 and October 2, 2020,

WSOU filed six separate infringement actions against Huawei involving six unrelated patents asserted against several unrelated products. *See* EX1100. These six lawsuits are concurrently pending in the Western District of Texas ("the Court") before the Honorable Judge Alan D. Albright. *Id*. The action involving the '962 patent was assigned Case No. 6:20-cv-00892 ("the Related Litigation"). The remaining six lawsuits are identified by different cases numbers and are not formally consolidated.

WSOU served its preliminary infringement contentions on February 5, 2021, but oddly characterized the contentions as "confidential" and did not authorize Huawei's in-house counsel to view the charts of the preliminary infringement contentions until February 24, 2021. *See* EX1101, 1. As such, this Petition was filed nine weeks later after initially learning of the asserted claims and about six weeks after actually viewing infringement charts. This Petition was served on Patent Owner even before Huawei's preliminary invalidity contentions, which are not due until April 12, 2021 (extended from April 7 upon agreement from the parties). *Id*.

The Court set a *Markman* hearing for August 12, 2021, and the parties are scheduled to exchange terms for construction on April 16, 2021. *See* EX1101, 2-3. Per the Court's default order, fact discovery will formally open on August 16, 2021, two business days after the *Markman* hearing. *See* EX1101, 3. In other words, little discovery—and certainly no meaningful expert discovery regarding

invalidity of the '962 patent under 35 U.S.C. §§ 102 and 103—will be completed at the time of the Board's institution decision here.

For purposes of planning earlier dates throughout discovery, etc., the Court set two placeholder trial dates—a first trial starting on September 26, 2022 for an unknown "first" subset of the six asserted patents and a subsequent trial for the "remaining consolidated cases" starting on a date that "will be determined." EX1101, 5. In other words, a jury trial is scheduled for September 26, 2022, but neither the Court nor any party knows which subset of the six asserted patents will be in "the first of the consolidated cases" for the trial on that date. *Id.* More specifically to the '962 patent at issue here, no party currently knows whether the '962 patent will be part of the "remaining consolidated cases" starting on a later (unknown) date after the Board's final written decision here. *Id.* Any allegation to the contrary is pure speculation..

Factor 1 (Stay)—No party in the Related Litigation has request a stay at this time. Huawei currently plans to seek a motion to stay after the Board's decision to institute IPR here because, in Judge Albright's court, a motion filed earlier would be premature. Again, the facts at play here are unique. There are six distinct lawsuits (asserting six unrelated patents) all unrealistically scheduled for trial on the same date. In such unique circumstances, it is unclear how Judge Albright would

rule on a motion to stay for the particular lawsuit involving the '962 patent, especially after IPR is instituted against the '962 patent months before the due date for Patent Owner to amend its complaint (December 2021) and long before expert reports/discovery (March 2022). This cloud of uncertainty means Factor 1 is neutral.

Factor 2 (Trial Date)—While the Court set September 26, 2022 as a placeholder trial date for an unknown "first" subset of the six asserted patents and a later (unknown) trial for the "remaining consolidated cases," it is far from certain whether the '962 patent will be part of the "first" trial or the later second trial. EX1101, 5. The only certainty at this time is that several of the six patents will not be part of the September 26, 2022 trial because they will be grouped into the "remaining consolidated cases." *Id.* Presently, there is no hint as to how the scheduling shuffle will play out, and it would be erroneous for any party to speculate that the '962 patent will necessarily be excluded from the "remaining consolidated cases." *Id.*

The *Fintiv* panel noted that the Board "generally take[s] courts' trial schedules at face value absent some strong evidence to the contrary." *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15, 13 (PTAB, "informative," May 13, 2020) ("*Fintiv II*"). For the reasons detailed above, such "strong evidence" exists on this record. Due to WSOU's litigation tactics, neither the Court nor any party knows

which one of the six asserted patents will be the subject of the trial starting on September 26, 2022. There is, in effect, no *certain* date for a jury trial that specifically addresses the '962 patent.

The "informative" guidance in *Sand Revolution* aligns with the facts of this case. *Sand Revolution*, IPR2019-01393, Paper 24 at 8-10. Even if Patent Owner (improperly) speculates the district court will necessarily insert the '962 patent into the "first" subset for a jury trial on September 26, 2022, the narrow gap in time between the jury's final verdict (end of September 2022 or later) and the Board's projected Final Written Decision (October 2022) is less than one month. The panel in *Sand Revolution*, also facing meaningful questions of uncertainty about the trial date, weighed Factor 2 "marginally" *against* denial with a three-month time gap. *Id.* The *Sand Revolution* guidance demonstrates the proper result when the district court's "evolving schedule" makes it "unclear" when the trial would be held. *Id.* A similar lack of clarity exists in this case but for a slightly different reason—there is significant uncertainty as to whether the '962 patent will be in the "first" subset for trial on September 26, 2022 or in the second subset of the "remaining consolidated cases" for trial at a later unknown date. EX1101, 5.

Similarly, the Board's analysis in *Google LLC, et al. v. Parus Holdings, Inc.* is compelling. *See* IPR2020-00846, Paper 9, 12-14 (PTAB Oct. 21, 2020). There, the district court reserved a broad range of "predicted" trial dates but declined to

specify further. *Id*. (noting a trial date range of July 12-30, 2021, and further noting the court's statement that it was "not going to pick a date right now"). With "only three months" between the range of trial dates and a final written decision, the Board deemed Factor 2 "neutral" based on "substantial uncertainty in the Texas court's 'Predicted Jury Selection/Trial' date." *Id*.

The less-than-a-month time gap presently at issue is narrower than *Sand Revolution* and the trial date uncertainty is comparable to *Google v. Parus*. The well-reasoned analysis by the Board in those two cases weighed Factor 2 against discretionary denial. A similar outcome is appropriate here.

Factor 3 (Investment)—The Related Litigation is currently in its infancy. Huawei has yet to serve its preliminary invalidity contentions, and the parties have yet to exchange proposed terms for construction. Huawei acted promptly in response to WSOU's identification of asserted claims in preliminary infringement contentions, filing this Petition only nine weeks after initially learning of the asserted claims and about six weeks after Huawei's in-house counsel was finally authorized to view the charts of the preliminary infringement contentions. *See* EX1101, 1.

At the projected date of institution (October 2021), the fact discovery period will have five more months of duration before the close of fact discovery (March 24, 2022), and expert reports/discovery will not even start until later (closing in

May 19, 2022). EX1101, 4. Beyond a *Markman* order, which is not dispositive here and is unrelated to the invalidity issues based upon the prior art publications cited in this Petition, the Court will have not issued any substantive orders relevant to invalidity based on prior art publications.

The facts here compare favorably to *Fintiv*. In that case, also co-pending with litigation at the Western District of Texas, the petitioner filed *five months* after receiving preliminary infringement contentions, but the petition here was filed less than eight weeks after receiving the asserted claim numbers (and less than five weeks after Patent Owner authorized Huawei's in-house counsel to view the claim charts). *See Fintiv II* at 9. There, "[a]t the time of filing the Petition, the parties were in the midst of preparations for the *Markman* hearing," while here, the parties have not even exchanged terms. *Id*.

The "informative" guidance in *Sand Revolution* is telling here too. By the time of institution in this proceeding, the Related Litigation will be at a similar posture where "aside from the district court's *Markman* Order, much of the district court's investment relates to ancillary matters untethered to the validity issue itself." *Sand Revolution*, IPR2019-01393, Paper 24, 10-11. The parallels are also notable because:

> [M]uch work remains in the district court case as it relates to invalidity: fact discovery is still ongoing, expert reports are not yet due, and substantive motion practice is yet to come.

Id. at 11 (internal citation omitted); *see also Fintiv I* at 10 ("If, at the time of the institution decision, the district court has not issued orders related to the patent at issue in the petition, this fact weighs against exercising discretion to deny institution"). In fact, the circumstances under Factor 3 here are similar to *Sotera*. *See Sotera Wireless, Inc. v. Masimo Corporation*, IPR2020-01019, Paper 12, 16-17 (PTAB Precedential Dec. 1, 2020) ("much other work remains in the parallel proceeding as it relates to invalidity" and the "explanation for timing of the Petition is reasonable, … particular in view of the large number of patents and claims"). In this case too, Factor 3 "weighs in favor of not exercising discretion to deny" as a result of "the relatively limited investment in the parallel proceeding to date" and "the fact that the timing of the Petitioner was reasonable." *Id.* at 17.

Factor 4 (Overlap)—As an initial matter, no party currently knows whether the '962 patent will be part of the "remaining consolidated cases" for second trial starting on a later (unknown) date after the Board's final written decision here. EX1101, 5; *supra*, Analysis of Factors 1-2. In such circumstances, there would be absolutely no overlap between invalidity grounds addressed in the Board's final written decision and in the later jury trial because 35 U.S.C. §315(e)(2) necessarily forbids it. Given the undefined nature of which one of the jury trials will actually include the '962 patent, these questions related to "overlap" in Factor 4 are, at best,

speculative.

Moreover, even if Patent Owner indulges in speculation to assume that the '962 patent will necessarily be part of the "first" subset of cases for trial on September 26, 2022 rather than in the later subset, Huawei's stipulation here "mitigates" concerns related to overlapping prior art grounds. *Sand Revolution*, IPR2019-01393, Paper 24, 11-12; *see* EX1102, 1 ("not pursue ... the same prior art grounds"). According this informative guidance, Factor 4 is weighs at least "marginally in favor not exercising discretion to deny IPR." *Sand Revolution*, IPR2019-01393, Paper 24, 12.

Factor 5 (Parties)—Because the parties here and at the District Court are the same, Factor 5 favors denial if trial precedes the Board's Final Written Decision and favors institution if the opposite is true (due to the 35 U.S.C. 315(e)(2) estoppel provision). *Google*, IPR2020-00846, Paper 9, 20-21 ("[W]e decline to speculate as to whether we are likely to address the challenged patent before the Texas court. Thus, [Factor 5] is neutral."). Neither circumstance can be confirmed in this case without improper speculation because the *actual* date of a jury trial involving the '962 patent is uncertain. EX1101, 5 (a later unknown trial for "the remaining consolidated cases"). Under these unique circumstances, Factor 5 is neutral.

Factor 6 (Merits and Other Circumstances)—The merits of this Petition are particularly strong. Section VII above presents two prior art grounds (Grounds

1-2) against the '962 patent's claims. As discussed, the prior art and arguments at issue here are materially different from those considered by the Examiner during prosecution. The strength of the merits alone is enough to outweigh any inefficiencies born of parallel litigation. *See Fintiv*, 15.

And there are additional circumstances that also favor institution, such as the effect on "the economy [and] the integrity of the patent system." *Consolidated Trial Practice Guide* ("*CTPG*"), 56 (quoting 35 U.S.C. § 316(b)). Relevant to the former, WSOU, an entity specializing in patent licensing and negotiation, is asserting the '962 patent's overbroad claims against Huawei's communication diversion service. *See* EX1009. Fully vetting an eighteen-year-old patent (filed 2003) only now asserted against Huawei's product would be beneficial to the economy.

The integrity of the patent system equally weighs in favor of institution. The analysis in Section VII of this Petition shows that the '962 patent's Challenged Claims are too broad, and the dubious prosecution record does not adequately explain why the Examiner issued a Notice of Allowance in the first place (*see supra* Section IV.B). AIA trials were intended to "improve patent quality and limit unnecessary and counterproductive litigation costs." *CTPG*, 56 (quoting H.R. Rep. No. 112-98, pt. 1, at 40 (2011)). This case provides an opportunity to fulfill those objectives. The quality of the '962 patent would undoubtedly be improved by cancelling the unpatentable claims presently under challenge. And such a result could

avert future litigation (and licensing) costs caused by WSOU's continued assertion efforts.

For all these reasons, Factor 6 and the *Fintiv* Factors as a whole strongly favor institution. Finally, Petitioner notes the ongoing legal challenge to discretionary denials of IPR based on the *Fintiv* and *NHK* precedential decisions (*e.g.*, *Apple Inc. et al. v. Iancu*, No. 5:20-cv-06128 (N.D. Cal.)), and reserves the opportunity to address the result of that case and any impact in this proceeding.

IX. CONCLUSION

Petitioner requests IPR of the Challenged Claims pursuant to Grounds 1-2.

Respectfully submitted,

Dated: April 9, 2021

/Kenneth J. Hoover/
Michael T. Hawkins, Reg. No. 57,867
Kenneth Hoover, Reg. No. 68,116

(Control No. IPR2021-00690)

Attorneys for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 10,801 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Respectfully submitted,

Dated: April 9, 2021

/Kenneth J. Hoover/
Michael T. Hawkins, Reg. No. 57,867
Kenneth Hoover, Reg. No. 68,116

Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on April 9, 2021, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided via Federal Express, to the Patent Owner by serving the correspondence address of record as follows:

SQUIRE PB
ATTN: IP Department
2550 M Street, NW
Washington DC 20037

/Edward G. Faeth/
Edward Faeth
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667